N.E.

(c) at each of a plurality of the distributed electronic devices, generating a partial result for the distributed cryptographic computation using at least one of said random values; and

(d) computing a final result for the distributed cryptographic computation using partial results.

Please add the following new claims.

Sub B2

12. A method of distributed cryptographic computation using a cryptographic value shared among a plurality of distributed electronic devices, said method comprising:

(a) computing shared values over a known and agreed context;

(b) generating random values using said shared values;

(c) at each of a plurality of the distributed electronic devices, generating a partial result for the cryptographic computation using a share of the cryptographic value and at least one of said random values; and

(d) computing a final result for the distributed cryptographic computation using partial results.

a1

13. The method of distributed cryptographic computation as recited by claim 1, wherein each shared value is shared among a subset of the distributed electronic devices.

B1

14. The method of distributed cryptographic computation as recited by claim 12, wherein each shared value is shared among a subset of the distributed electronic devices.

15. The method of distributed cryptographic computation as recited by claim 1, wherein each of a plurality of shared values is shared among a distinct subset of the distributed electronic devices.

16. The method of distributed cryptographic computation as recited by claim 12, wherein each of a plurality of shared values is shared among a distinct subset of the distributed electronic devices.

Sub B3

17. The method of distributed cryptographic computation as recited by claim 1, wherein each of a plurality of shared values is shared among a pair of the distributed electronic devices.

18. The method of distributed cryptographic computation as recited by claim 12, wherein each of a plurality of shared values is shared among a pair of the distributed electronic devices.

a'

19. The method of distributed cryptographic computation as recited by claim 1, wherein each of a plurality of shared values is shared among a distinct pair of the distributed electronic devices.

20. The method of distributed cryptographic computation as recited by claim 12, wherein each of a plurality of shared values is shared among a distinct pair of the distributed electronic devices.

21. The method of distributed cryptographic computation as recited by claim 1, wherein each of a plurality of shared values is (a) shared among a distinct subset of distributed electronic devices and (b) used to generate a partial result in a way that permits verification of correctness of a partial result.

a1

22. The method of distributed cryptographic computation as recited by claim 12, wherein each of a plurality of shared values is (a) shared among a distinct subset of distributed electronic devices and (b) used to generate a partial result in a way that permits verification of correctness of a partial result.--